

CLAIMS

What is claimed is:

- 1 1. An apparatus comprising:
 - 2 an interface to map a device via a bus to an address space of a chipset in
 - 3 a secure environment for an isolated execution mode, the secure environment
 - 4 being associated with an isolated memory area accessible by at least one
 - 5 processor, the at least one processor operating in one of a normal execution
 - 6 mode and the isolated execution mode; and
 - 7 a communication storage corresponding to the address space to allow the
 - 8 device to exchange security information with the at least one processor in the
 - 9 isolated execution mode in a remote attestation.
- 1 2. The apparatus of claim 1 wherein the security information includes
- 2 at least one of a static public key and a static key certificate.
- 1 3. The apparatus of claim 2 wherein the interface comprises:
 - 2 a decoder to decode the address space onto the bus so that an access to
 - 3 the chipset is passed to the device.
- 1 4. The apparatus of claim 3 wherein the device accesses a chipset
- 2 storage via the address space.

1 5. The apparatus of claim 4 wherein the communication storage
2 comprises:

3 a configuration storage to store device configuration information.

1 6. The apparatus of claim 5 wherein the communication storage
2 further comprises:

3 a status register to store device status of the device;

4 a command register to store a device command for a command interface
5 set; and

6 an input/output block (IOB) to store input and output data corresponding
7 to the command.

1 7. The apparatus of claim 6 wherein the configuration storage
2 comprises:

3 a public key storage to store the static public key;

4 a key certificate storage to store the static key certificate; and

5 an interface set storage to store an interface set identifier, the interface
6 set identifier identifying a command interface set supported by the device.

1 17. The apparatus of claim 16 wherein the chipset parameter is one of
2 a chipset isolated nub loader hash, a chipset isolated hash log, a software hash,
3 and a nonce.

1 18. The apparatus of claim 17 wherein the chipset isolated nub loader
2 hash and the chipset isolated hash log are stored in the chipset storage.

1 19. The apparatus of claim 18 wherein the software hash and the
2 nonce are provided by a process nub.

1 20. The apparatus of claim 3 wherein the device accesses a remote
2 server via the address space.

1 21. A method comprising:
2 mapping a device via a bus to an address space of a chipset in a secure
3 environment for an isolated execution mode, the secure environment being
4 associated with an isolated memory area accessible by at least one processor,
5 the at least one processor operating in one of a normal execution mode and the
6 isolated execution mode; and

3 performing a device command corresponding to a command interface set
4 to a command register; and
5 storing input and output data corresponding to the command in an
6 input/output block (IOB).

1 27. The method of claim 26 wherein storing in the configuration storage
2 comprises:

3 storing the static public key in a public key storage;

4 storing the static key certificate in a key certificate storage; and

5 storing an interface set identifier in an interface set storage, the interface
6 set identifier identifying a command interface set supported by the device.

1 28. The method of claim 27 wherein storing in the configuration storage
2 further comprises:

3 storing a manufacturer identifier in a manufacturer identifier storage; and

4 storing a revision identifier in a revision storage.

1 29. The method of claim 27 wherein performing the device command
2 comprises performing a reset command and a connect command corresponding
3 to an initialization set.

1 30. The method of claim 27 wherein performing the device command
2 comprises performing at least one of a public key enumeration, a key certificate
3 enumeration, and a signing operation, the public key enumeration, the key
4 certificate enumeration, and the signing operation corresponding to an
5 attestation set.

1 31. The method of claim 30 wherein storing the device status
2 comprises:

3 providing a connection status to indicate that the device is responsive to
4 the connect command; and

5 providing an estimate of processing time for an operation specified in the
6 command.

1 32. The method of claim 31 wherein storing the device status further
2 comprises:

3 indicating status of a self test in response to the reset command.

1 33. The method of claim 30 wherein performing the public key
2 enumeration comprises enumerating an additional public key other than the
3 static public key.

1 34. The method of claim 30 wherein performing the key certificate
2 enumeration comprises enumerating an additional key certificate other than the
3 static key certificate.

1 35. The method of claim 30 wherein performing the sign operation
2 comprises generating a signature to attest validity of the secure environment
3 using a private key provided by the chipset.

1 36. The method of claim 35 wherein the signature corresponds to
2 signing a chipset parameter.

1 37. The method of claim 36 wherein the chipset parameter is one of a
2 chipset isolated nub loader hash, a chipset isolated hash log, a software hash,
3 and a nonce.

1 38. The method of claim 37 wherein the chipset isolated nub loader
2 hash and the chipset isolated hash log are stored in the chipset storage.

3 computer readable program code for storing device status of the device in
4 a status register;

5 computer readable program code for performing a device command
6 corresponding to a command interface set to a command register; and

7 computer readable program code for storing input and output data
8 corresponding to the command in an input/output block (IOB).

1 47. The computer program product of claim 46 wherein the computer
2 readable program code for storing in the configuration storage comprises:

3 computer readable program code for storing the static public key in a
4 public key storage;

5 computer readable program code for storing the static key certificate in a
6 key certificate storage; and

7 computer readable program code for storing an interface set identifier in
8 an interface set storage, the interface set identifier identifying a command
9 interface set supported by the device.

1 48. The computer program product of claim 47 wherein the computer
2 readable program code for storing in the configuration storage further comprises:

3 computer readable program code for storing a manufacturer identifier in a
4 manufacturer identifier storage; and

5 computer readable program code for storing a revision identifier in a
6 revision storage.

1 49. The computer program product of claim 47 wherein the computer
2 readable program code for performing the device command comprises
3 performing a reset command and a connect command corresponding to an
4 initialization set.

1 50. The computer program product of claim 47 wherein the computer
2 readable program code for performing the device command comprises
3 performing at least one of a public key enumeration, a key certificate
4 enumeration, and a signing operation, the public key enumeration, the key
5 certificate enumeration, and the signing operation corresponding to an
6 attestation set.

1 51. The computer program product of claim 50 wherein the computer
2 readable program code for storing the device status comprises:

3 computer readable program code for providing a connection status to
4 indicate that the device is responsive to the connect command; and

5 computer readable program code for providing an estimate of processing
6 time for an operation specified in the command.

1 57. The computer program product of claim 56 wherein the chipset
2 parameter is one of a chipset isolated nub loader hash, a chipset isolated hash
3 log, a software hash, and a nonce.

1 58. The computer program product of claim 57 wherein the chipset
2 isolated nub loader hash and the chipset isolated hash log are stored in the
3 chipset storage.

1 59. The computer program product of claim 58 wherein the software
2 hash and the nonce are provided by a process nub.

1 60. The computer program product of claim 43 wherein the device
2 accesses a remote server via the address space.

1 61. A system comprising:

2 at least one processor operating in a secure environment, the at least one
3 processor having one of a normal execution mode and an isolated execution
4 mode;

5 a memory coupled to the at least one processor, the memory having an
6 isolated memory area accessible to the at least one processor in the isolated
7 execution mode; and

8 a chipset coupled to the at least one processor and the memory, the
9 chipset having a circuit, the circuit comprising:

10 an interface to map a device via a bus to an address space of the
11 chipset in the secure environment, and

12 a communication storage corresponding to the address space to
13 allow the device to exchange security information with the at least
14 one processor in the isolated execution mode in a remote
15 attestation.

1 62. The system of claim 61 wherein the security information includes at
2 least one of a static public key and a static key certificate.

1 63. The system of claim 62 wherein the interface comprises:

2 a decoder to decode the address space onto the bus so that an access to
3 the chipset is passed to the device.

1 64. The system of claim 63 wherein the device accesses a chipset
2 storage via the address space.

1 65. The system of claim 64 wherein the communication storage
2 comprises:
3 a configuration storage to store device configuration information.

1 66. The system of claim 65 wherein the communication storage further
2 comprises:
3 a status register to store device status of the device;
4 a command register to store a device command for a command interface
5 set; and
6 an input/output block (IOB) to store input and output data corresponding
7 to the command.

1 67. The system of claim 66 wherein the configuration storage
2 comprises:
3 a public key storage to store the static public key;
4 a key certificate storage to store the static key certificate; and
5 an interface set storage to store an interface set identifier, the interface
6 set identifier identifying a command interface set supported by the device.

